

H. Tanno et al.

11/25/03

Q 78595

1071

日 本 国 特 許 庁  
JAPAN PATENT OFFICE

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office.

出 願 年 月 日  
Date of Application: 2 0 0 2 年 1 1 月 2 6 日

出 願 番 号  
Application Number: 特 願 2 0 0 2 - 3 4 2 7 3 5

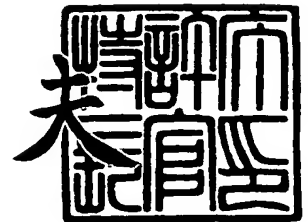
[ST. 10/C]: [ J P 2 0 0 2 - 3 4 2 7 3 5 ]

出 願 人  
Applicant(s): 日 本 電 気 株 式 会 社  
エヌイーシーシステムテクノロジー株式会社

2 0 0 3 年 8 月 2 0 日

特許庁長官  
Commissioner,  
Japan Patent Office

今 井 康 夫



出証番号 出証特 2 0 0 3 - 3 0 6 8 0 2 3

【書類名】 特許願  
【整理番号】 64300936  
【提出日】 平成14年11月26日  
【あて先】 特許庁長官 太田 信一郎 殿  
【国際特許分類】 G06F 17/30  
G06F 17/60  
【発明者】  
【住所又は居所】 東京都港区芝五丁目 7 番 1 号 日本電気株式会社内  
【氏名】 丹野 秀和  
【発明者】  
【住所又は居所】 東京都港区芝五丁目 7 番 1 号 日本電気株式会社内  
【氏名】 関 義長  
【発明者】  
【住所又は居所】 大阪府大阪市中心区城見一丁目 4 番 2 4 号 エヌイーシー  
システムテクノロジー株式会社内  
【氏名】 長谷井 伸次  
【特許出願人】  
【識別番号】 000004237  
【氏名又は名称】 日本電気株式会社  
【特許出願人】  
【識別番号】 390001395  
【氏名又は名称】 エヌイーシーシステムテクノロジー株式会社  
【代理人】  
【識別番号】 100086759  
【弁理士】  
【氏名又は名称】 渡辺 喜平  
【手数料の表示】  
【予納台帳番号】 013619  
【納付金額】 21,000円

【提出物件の目録】

【物件名】 明細書 1

【物件名】 図面 1

【物件名】 要約書 1

【包括委任状番号】 9001716

【包括委任状番号】 9005478

【プルーフの要否】 要

【書類名】 明細書

【発明の名称】 ネットワークを利用したソフトウェア資産管理漏れ検出方法、システム、サーバ、及びプログラム

【特許請求の範囲】

【請求項 1】 コンピュータごとに、その基本情報及びインストールされているソフトウェア、修正パッチの適用状況を管理するソフトウェア資産管理から漏れているコンピュータを検出するためのネットワークを利用したソフトウェア資産管理漏れ検出方法であって、

所定のネットワークに接続された全てのコンピュータについて、各コンピュータを特定するための情報を保有するネットワーク接続コンピュータリストと、前記ソフトウェア資産管理の管理対象となっている全てのコンピュータについて、各コンピュータを特定するための情報を保有するソフトウェア資産管理リストとにもとづいて、前記ネットワーク接続コンピュータリストに存在し、かつ、前記ソフトウェア資産管理リストに存在しないコンピュータを抽出し、ソフトウェア資産管理漏れのコンピュータのリストを作成する

ことを特徴とするネットワークを利用したソフトウェア資産管理漏れ検出方法。

【請求項 2】 請求項 1 記載のネットワークを利用したソフトウェア資産管理漏れ検出方法において、

前記ネットワーク接続コンピュータリスト及び前記ソフトウェア資産管理リストにもとづいて、前記ソフトウェア資産管理リストに存在し、かつ、前記ネットワーク接続コンピュータリストに存在しないコンピュータを抽出し、非使用状態となっているコンピュータのリストを作成する

ことを特徴とするネットワークを利用したソフトウェア資産管理漏れ検出方法。

【請求項 3】 コンピュータごとに、その基本情報及びインストールされているソフトウェア、修正パッチの適用状況を管理するソフトウェア資産管理から漏れているコンピュータを検出するためのネットワークを利用したソフトウェア資産管理漏れ検出システムであって、

所定のネットワークに接続された全てのコンピュータについて、各コンピュータを特定するための情報を保有するネットワーク接続コンピュータリストを備えたネットワーク接続管理サーバと、

前記ソフトウェア資産管理の管理対象となっている全てのコンピュータについて、各コンピュータを特定するための情報を保有するソフトウェア資産管理リストを備えたソフトウェア資産管理サーバと、

前記ネットワーク接続コンピュータリスト及び前記ソフトウェア資産管理リストにもとづいて、前記ネットワーク接続コンピュータリストに存在し、かつ、前記ソフトウェア資産管理リストに存在しないコンピュータを抽出し、ソフトウェア資産管理漏れのコンピュータのリストを作成するソフトウェア資産管理漏れ検出サーバとを有する

ことを特徴とするネットワークを利用したソフトウェア資産管理漏れ検出システム。

【請求項4】 請求項3記載のネットワークを利用したソフトウェア資産管理漏れ検出システムにおいて、

前記ソフトウェア資産管理漏れ検出サーバが、

前記ネットワーク接続コンピュータリスト及び前記ソフトウェア資産管理リストにもとづいて、前記ソフトウェア資産管理リストに存在し、かつ、前記ネットワーク接続コンピュータリストに存在しないコンピュータを抽出し、非使用状態となっているコンピュータのリストを作成する

ことを特徴とするネットワークを利用したソフトウェア資産管理漏れ検出システム。

【請求項5】 コンピュータごとに、その基本情報及びインストールされているソフトウェア、修正パッチの適用状況を管理するソフトウェア資産管理から漏れているコンピュータを検出するためのネットワークを利用したソフトウェア資産管理漏れ検出サーバであって、

所定のネットワークに接続された全てのコンピュータについて、各コンピュータを特定するための情報を保有するネットワーク接続コンピュータリストを備えたネットワーク接続管理サーバから、前記ネットワーク接続コンピュータリスト

を受信するとともに、

前記ソフトウェア資産管理の管理対象となっている全てのコンピュータについて、各コンピュータを特定するための情報を保有するソフトウェア資産管理リストを備えたソフトウェア資産管理サーバから、前記ソフトウェア資産管理リストを受信し、

前記ネットワーク接続コンピュータリスト及び前記ソフトウェア資産管理リストにもとづいて、前記ネットワーク接続コンピュータリストに存在し、かつ、前記ソフトウェア資産管理リストに存在しないコンピュータを抽出し、ソフトウェア資産管理漏れのコンピュータのリストを作成する

ことを特徴とするネットワークを利用したソフトウェア資産管理漏れ検出サーバ。

【請求項6】 コンピュータごとに、その基本情報及びインストールされているソフトウェア、修正パッチの適用状況を管理するソフトウェア資産管理から漏れているコンピュータを検出するためのネットワークを利用したソフトウェア資産管理漏れ検出サーバであって、

所定のネットワークに接続された全てのコンピュータについて、各コンピュータを特定するための情報を保有するネットワーク接続コンピュータリストを作成するネットワーク接続管理部と、

前記ソフトウェア資産管理の管理対象となっている全てのコンピュータについて、各コンピュータを特定するための情報を保有するソフトウェア資産管理リストを作成するソフトウェア資産管理部と、

前記ネットワーク接続管理部から入力した前記ネットワーク接続コンピュータリスト及び前記ソフトウェア資産管理部から入力した前記ソフトウェア資産管理リストにもとづいて、前記ネットワーク接続コンピュータリストに存在し、かつ、前記ソフトウェア資産管理リストに存在しないコンピュータを抽出し、ソフトウェア資産管理漏れのコンピュータのリストを作成するソフトウェア資産管理漏れ検出部とを有する

ことを特徴とするネットワークを利用したソフトウェア資産管理漏れ検出サーバ。

【請求項 7】 請求項 5 記載のネットワークを利用したソフトウェア資産管理漏れ検出サーバが、

前記ネットワーク接続コンピュータリスト及び前記ソフトウェア資産管理リストにもとづいて、前記ソフトウェア資産管理リストに存在し、かつ、前記ネットワーク接続コンピュータリストに存在しないコンピュータを抽出し、非使用状態となっているコンピュータのリストを作成する

ことを特徴とするネットワークを利用したソフトウェア資産管理漏れ検出サーバ。

【請求項 8】 請求項 6 記載のネットワークを利用したソフトウェア資産管理漏れ検出サーバにおいて、

前記ソフトウェア資産管理漏れ検出部が、

前記ネットワーク接続コンピュータリスト及び前記ソフトウェア資産管理リストにもとづいて、前記ソフトウェア資産管理リストに存在し、かつ、前記ネットワーク接続コンピュータリストに存在しないコンピュータを抽出し、非使用状態となっているコンピュータのリストを作成する

ことを特徴とするネットワークを利用したソフトウェア資産管理漏れ検出サーバ。

【請求項 9】 請求項 5～8 のいずれかに記載のネットワークを利用したソフトウェア資産管理漏れ検出サーバが、

前記ネットワーク接続コンピュータリスト及び前記ソフトウェア資産管理リストをソートし、このソートしたネットワーク接続コンピュータリスト及びソフトウェア資産管理リストにもとづいて、前記ソフトウェア資産管理漏れのコンピュータのリスト、又は、前記非使用状態となっているコンピュータのリストを作成する

ことを特徴とするネットワークを利用したソフトウェア資産管理漏れ検出サーバ。

【請求項 10】 コンピュータごとに、その基本情報及びインストールされているソフトウェア、修正パッチの適用状況を管理するソフトウェア資産管理から漏れているコンピュータを検出するためのネットワークを利用したソフトウェ

ア資産管理漏れ検出プログラムであって、

ソフトウェア資産管理漏れ検出サーバに、

所定のネットワークに接続された全てのコンピュータについて、各コンピュータを特定するための情報を保有するネットワーク接続コンピュータリストを備えたネットワーク接続管理サーバから、前記ネットワーク接続コンピュータリストを受信させるとともに、

前記ソフトウェア資産管理の管理対象となっている全てのコンピュータについて、各コンピュータを特定するための情報を保有するソフトウェア資産管理リストを備えたソフトウェア資産管理サーバから、前記ソフトウェア資産管理リストを受信させ、

前記ネットワーク接続コンピュータリスト及び前記ソフトウェア資産管理リストにもとづいて、前記ネットワーク接続コンピュータリストに存在し、かつ、前記ソフトウェア資産管理リストに存在しないコンピュータを抽出させ、ソフトウェア資産管理漏れのコンピュータのリストを作成させる

ことを特徴とするネットワークを利用したソフトウェア資産管理漏れ検出プログラム。

【請求項 11】 コンピュータごとに、その基本情報及びインストールされているソフトウェア、修正パッチの適用状況を管理するソフトウェア資産管理から漏れているコンピュータを検出するためのネットワークを利用したソフトウェア資産管理漏れ検出プログラムであって、

ソフトウェア資産管理漏れ検出サーバに、

所定のネットワークに接続された全てのコンピュータについて、各コンピュータを特定するための情報を保有するネットワーク接続コンピュータリストを作成させるとともに、

前記ソフトウェア資産管理の管理対象となっている全てのコンピュータについて、各コンピュータを特定するための情報を保有するソフトウェア資産管理リストを作成させ、

前記ネットワーク接続コンピュータリスト及び前記ソフトウェア資産管理リストにもとづいて、前記ネットワーク接続コンピュータリストに存在し、かつ、前



記ソフトウェア資産管理リストに存在しないコンピュータを抽出させ、ソフトウェア資産管理漏れのコンピュータのリストを作成させる

ことを特徴とするネットワークを利用したソフトウェア資産管理漏れ検出プログラム。

【請求項 12】 請求項 10 又は 11 記載のネットワークを利用したソフトウェア資産管理漏れ検出プログラムが、

ソフトウェア資産管理漏れ検出サーバに、

前記ネットワーク接続コンピュータリスト及び前記ソフトウェア資産管理リストにもとづいて、前記ソフトウェア資産管理リストに存在し、かつ、前記ネットワーク接続コンピュータリストに存在しないコンピュータを抽出させ、非使用状態となっているコンピュータのリストを作成させる

ことを特徴とするネットワークを利用したソフトウェア資産管理漏れ検出プログラム。

【請求項 13】 請求項 10～12 のいずれかに記載のネットワークを利用したソフトウェア資産管理漏れ検出プログラムが、

ソフトウェア資産管理漏れ検出サーバに、

前記ネットワーク接続コンピュータリスト及び前記ソフトウェア資産管理リストをソートさせ、このソートされたネットワーク接続コンピュータリスト及びソフトウェア資産管理リストにもとづいて、前記ソフトウェア資産管理漏れのコンピュータのリスト、又は、前記非使用状態となっているコンピュータのリストを作成させる

ことを特徴とするネットワークを利用したソフトウェア資産管理漏れ検出プログラム。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】

本発明は、コンピュータごとに、その基本情報及びインストールされているソフトウェア、修正パッチの適用状況を管理するソフトウェア資産管理から、管理すべきコンピュータが漏れることを防止するネットワークを利用したソフトウェ

ア資産管理漏れ検出方法、システム、サーバ及びプログラムに関する。

#### 【0002】

##### 【従来の技術】

近年、コンピュータは、企業や団体などにおいて、その業務上広く使用されている。このコンピュータの使用にあたっては、その使用の目的にあったソフトウェアを用いる必要があるため、これらの企業等は、コンピュータに様々なソフトウェアをインストールして使用している。

そのため、企業等においては、購入したソフトウェアライセンスを適切に管理し、組織内で不正にソフトウェアをコピーして利用されることのないような施策を講じる必要がある。

しかし、ソフトウェアはほとんどの場合、ひとつの媒体から複数のコンピュータに簡単にインストールすることが可能であるため、ライセンス数を超えてインストールされていないかどうかを正確に把握する作業は膨大なものになり、また調査した結果を維持管理することも組織が大きくなるにつれて非常に困難なものになるという問題があった。

#### 【0003】

また、最近ではコンピュータの多くがネットワークに接続され、ネットワークを介して情報のやり取りが行われている。

このような状況においては、電子メールやWebアクセスなどを媒介とするウィルスの感染を防ぐために、ネットワークに接続されているコンピュータにインストールされているOSやアプリケーションソフトウェアが、ソフトウェアの開発元が提供している修正パッチを適用することなどによってセキュリティ上問題がない状態になっているかを管理する必要がある。

しかし、ソフトウェアライセンス管理の問題と同様に、OSやアプリケーションが適切に更新されているかどうかを把握するには非常に多大な作業が必要となるという問題があった。

#### 【0004】

これらの問題に対し、ネットワークに接続されている各コンピュータ上で、コンピュータの基本情報（ホスト名、ネットワークアドレス等）やインストールさ

れているソフトウェアのリスト情報等を収集するソフトウェア資産管理用のクライアントソフトウェアを動作させ、収集した情報をソフトウェア資産管理用のサーバに送信することにより、ソフトウェア資産情報が自動的に一元管理されるようにすることを可能とする方法等が提案されている（例えば、特許文献1～3参照。）。また、ソフトウェアの修正パッチを専用のサーバで管理し、コンピュータがパッチ未使用の場合に自動的に修正パッチをダウンロードして適用する方法等が提案されている（例えば、特許文献4，5参照。）

## 【0005】

## 【特許文献1】

特開2001-222424号公報

## 【特許文献2】

特開2001-290937号公報

## 【特許文献3】

特開2002-279165号公報

## 【特許文献4】

特開2000-250743号公報

## 【特許文献5】

特開2002-55839号公報

## 【0006】

## 【発明が解決しようとする課題】

しかしながら、このような従来の方法では、各コンピュータ上でソフトウェア資産管理用のクライアントソフトウェアや、修正パッチをダウンロードして適用するクライアントソフトウェアがインストールされ動作していること、又はOSやアプリケーションソフトウェアがこのようなクライアントソフトウェアと同等の機能を有していることが前提となっており、クライアントソフトウェアが動作していないコンピュータはソフトウェア資産管理情報から漏れてしまい、ソフトウェアの不正利用を見過ごしたり、セキュリティ上問題のある状態のコンピュータを見過ごしたりする恐れがあるという問題があった。

## 【0007】

本発明は、上記の事情にかんがみなされたものであり、コンピュータごとに、その基本情報及びインストールされているソフトウェア、修正パッチの適用状況を管理するソフトウェア資産管理から、管理すべきコンピュータが漏れることを防止することによって、OSやアプリケーションのパッチ適用状態が不明でセキュリティ上問題のある可能性の高いコンピュータを検出することを可能とするネットワークを利用したソフトウェア資産管理漏れ検出方法、システム、サーバ及びプログラムの提供を目的とする。

#### 【0008】

##### 【課題を解決するための手段】

上記目的を達成するため、本発明の請求項1記載のネットワークを利用したソフトウェア資産管理漏れ検出方法は、コンピュータごとに、その基本情報及びインストールされているソフトウェア、修正パッチの適用状況を管理するソフトウェア資産管理から漏れているコンピュータを検出するためのネットワークを利用したソフトウェア資産管理漏れ検出方法であって、所定のネットワークに接続された全てのコンピュータについて、各コンピュータを特定するための情報を保有するネットワーク接続コンピュータリストと、ソフトウェア資産管理の管理対象となっている全てのコンピュータについて、各コンピュータを特定するための情報を保有するソフトウェア資産管理リストとにもとづいて、ネットワーク接続コンピュータリストに存在し、かつ、ソフトウェア資産管理リストに存在しないコンピュータを抽出し、ソフトウェア資産管理漏れのコンピュータのリストを作成する方法としてある。

#### 【0009】

ネットワークを利用したソフトウェア資産管理漏れ検出方法をこのような方法にすれば、ソフトウェア資産管理情報とは別にネットワークに接続されているコンピュータを漏れなく含むリストを作成し、ネットワークアドレスなどネットワーク上でコンピュータを一意に識別することが可能な情報を用いることで、ソフトウェア資産管理から漏れているコンピュータを見つけ出すことができる。

このため、ソフトウェア資産管理から漏れているコンピュータを容易に洗い出すことが可能となる。

## 【0010】

また、ネットワークに接続されているコンピュータを漏れなく含むリストを作成する手段を、従来のソフトウェア資産管理システムから独立して構成し、ソフトウェア資産管理漏れのコンピュータを検出することができる。

そして、このソフトウェア資産管理漏れのコンピュータに対して、従来のソフトウェア資産管理システムを適用することが可能となる。

このため、従来のソフトウェア資産管理システムを大幅に変更することなくソフトウェア資産管理情報の漏れを防止することが可能となる。

## 【0011】

その結果、OSやソフトウェアのバージョンやパッチ適用状態等も同時に管理するソフトウェア資産管理において、ネットワークに接続されたコンピュータを漏れなく含んだリストを用いることによって、管理漏れを防ぐことが可能となる。

このため、OSやソフトウェアのバージョンやパッチ適用状態等が不明なコンピュータを検出し、パッチ適用状態が最新ではなくセキュリティホールとなりうるコンピュータがネットワークに接続されたままになることを防止することが可能となる。

## 【0012】

また、ネットワーク接続コンピュータリストとソフトウェア資産管理リストを1日ごとなど適切な間隔で定期的に更新して比較することにより、新規にネットワークに接続されたコンピュータがソフトウェア資産管理下にあるかどうかを確認することができる。

このため、ソフトウェア資産管理外のコンピュータや不正なコンピュータが接続された場合、管理外コンピュータとして早期に発見することが可能となる。

## 【0013】

なお、基本情報とは、ネットワークアドレスやコンピュータ名等の情報を意味している。また、この基本情報としては、各コンピュータを特定するための一の情報のみであってもかまわない。

また、所定のネットワークとは、例えば、社内LANやVPNなどであり、企

業や官公庁、学校、その他の団体や個人等によって、その管理の対象とされるネットワークを意味している。

【0014】

本発明の請求項2記載のネットワークを利用したソフトウェア資産管理漏れ検出方法は、請求項1記載のネットワークを利用したソフトウェア資産管理漏れ検出方法において、ネットワーク接続コンピュータリスト及びソフトウェア資産管理リストにもとづいて、ソフトウェア資産管理リストに存在し、かつ、ネットワーク接続コンピュータリストに存在しないコンピュータを抽出し、非使用状態となっているコンピュータのリストを作成する方法としてある。

【0015】

ネットワークを利用したソフトウェア資産管理漏れ検出方法をこのような方法にすれば、非使用コンピュータリストを作成することができるため、以前使用されていたが、現在は使用されていないコンピュータを洗い出すことが可能となる。

また、ソフトウェア資産管理漏れ検出リストと非使用コンピュータリストの双方を作成することによって、ソフトウェア資産管理から漏れているコンピュータを検出することができるとともに、現在未使用のソフトウェアの一覧を取得することも可能となり、ソフトウェア資産管理をより厳密に行うことが容易となる。

【0016】

本発明の請求項3記載のネットワークを利用したソフトウェア資産管理漏れ検出システムは、コンピュータごとに、その基本情報及びインストールされているソフトウェア、修正パッチの適用状況を管理するソフトウェア資産管理から漏れているコンピュータを検出するためのネットワークを利用したソフトウェア資産管理漏れ検出システムであって、所定のネットワークに接続された全てのコンピュータについて、各コンピュータを特定するための情報を保有するネットワーク接続コンピュータリストを備えたネットワーク接続管理サーバと、ソフトウェア資産管理の管理対象となっている全てのコンピュータについて、各コンピュータを特定するための情報を保有するソフトウェア資産管理リストを備えたソフトウェア資産管理サーバと、ネットワーク接続コンピュータリスト及びソフトウェア

資産管理リストにもとづいて、ネットワーク接続コンピュータリストに存在し、かつ、ソフトウェア資産管理リストに存在しないコンピュータを抽出し、ソフトウェア資産管理漏れのコンピュータのリストを作成するソフトウェア資産管理漏れ検出サーバとを有する構成としてある。

#### 【0017】

ネットワークを利用したソフトウェア資産管理漏れ検出システムをこのような構成にすれば、ソフトウェア資産管理サーバにより管理されるソフトウェア資産管理リストと、ネットワーク接続管理サーバによって作成されたネットワーク接続コンピュータリストにもとづいて、ネットワークアドレスなどネットワーク上でコンピュータを一意に識別することが可能な情報を用いることで、ネットワークに接続されているにもかかわらず、ソフトウェア資産管理が行われていないコンピュータを容易に見つけ出すことが可能となる。

その結果、OSやソフトウェアのバージョンやパッチ適用状態等が不明なコンピュータを検出し、パッチ適用状態が最新ではなくセキュリティホールとなりうるコンピュータがネットワークに接続されたままになることを防止することが可能となる。

#### 【0018】

また、ネットワークを利用したソフトウェア資産管理漏れ検出システムをこのような構成にすることによって、従来のソフトウェア資産管理システムに対して、大きな変更を行うことなく、その管理対象の漏れを防止することが可能となる。

さらに、ソフトウェア資産管理外のコンピュータや不正なコンピュータが接続された場合に、管理外のコンピュータとして早期に発見することも可能となる。

#### 【0019】

本発明の請求項4記載のネットワークを利用したソフトウェア資産管理漏れ検出システムは、請求項3記載のネットワークを利用したソフトウェア資産管理漏れ検出システムにおいて、ソフトウェア資産管理漏れ検出サーバが、ネットワーク接続コンピュータリスト及びソフトウェア資産管理リストにもとづいて、ソフトウェア資産管理リストに存在し、かつ、ネットワーク接続コンピュータリスト

に存在しないコンピュータを抽出し、非使用状態となっているコンピュータのリストを作成する構成としてある。

#### 【0020】

ネットワークを利用したソフトウェア資産管理漏れ検出システムをこのような構成にすれば、以前使用されていたが、現在は使用されていないコンピュータを洗い出すことが可能となる。

このため、ソフトウェア資産管理から漏れているコンピュータを検出することに加え、現在未使用のソフトウェアの一覧を取得することも可能となる。

#### 【0021】

本発明の請求項5記載のネットワークを利用したソフトウェア資産管理漏れ検出サーバは、コンピュータごとに、その基本情報及びインストールされているソフトウェア、修正パッチの適用状況を管理するソフトウェア資産管理から漏れているコンピュータを検出するためのネットワークを利用したソフトウェア資産管理漏れ検出サーバであって、所定のネットワークに接続された全てのコンピュータについて、各コンピュータを特定するための情報を保有するネットワーク接続コンピュータリストを備えたネットワーク接続管理サーバから、ネットワーク接続コンピュータリストを受信するとともに、ソフトウェア資産管理の管理対象となっている全てのコンピュータについて、各コンピュータを特定するための情報を保有するソフトウェア資産管理リストを備えたソフトウェア資産管理サーバから、ソフトウェア資産管理リストを受信し、ネットワーク接続コンピュータリスト及びソフトウェア資産管理リストにもとづいて、ネットワーク接続コンピュータリストに存在し、かつ、ソフトウェア資産管理リストに存在しないコンピュータを抽出し、ソフトウェア資産管理漏れのコンピュータのリストを作成する構成としてある。

#### 【0022】

ネットワークを利用したソフトウェア資産管理漏れ検出サーバをこのような構成にすれば、ネットワーク接続管理サーバからのネットワーク接続コンピュータリストと、ソフトウェア資産管理サーバからのソフトウェア資産管理リストにもとづいて、容易にソフトウェア資産管理漏れのコンピュータを検出することが可



能となる。

また、従来のソフトウェア資産管理システムが、ソフトウェア資産管理サーバに保有されている場合であっても、このソフトウェア資産管理サーバに対する変更をほとんど加える必要がない。

さらに、セキュリティホールとなりうるコンピュータがネットワークに接続されたままになることを防止し、ソフトウェア資産管理外のコンピュータや不正なコンピュータが接続された場合は、これを早期に発見することが可能となる。

#### 【0023】

本発明の請求項6記載のネットワークを利用したソフトウェア資産管理漏れ検出サーバは、コンピュータごとに、その基本情報及びインストールされているソフトウェア、修正パッチの適用状況を管理するソフトウェア資産管理から漏れているコンピュータを検出するためのネットワークを利用したソフトウェア資産管理漏れ検出サーバであって、所定のネットワークに接続された全てのコンピュータについて、各コンピュータを特定するための情報を保有するネットワーク接続コンピュータリストを作成するネットワーク接続管理部と、ソフトウェア資産管理の管理対象となっている全てのコンピュータについて、各コンピュータを特定するための情報を保有するソフトウェア資産管理リストを作成するソフトウェア資産管理部と、ネットワーク接続管理部から入力したネットワーク接続コンピュータリスト及びソフトウェア資産管理部から入力したソフトウェア資産管理リストにもとづいて、ネットワーク接続コンピュータリストに存在し、かつ、ソフトウェア資産管理リストに存在しないコンピュータを抽出し、ソフトウェア資産管理漏れのコンピュータのリストを作成するソフトウェア資産管理漏れ検出部とを有する構成としてある。

#### 【0024】

ネットワークを利用したソフトウェア資産管理漏れ検出サーバをこのような構成にすれば、一台のサーバにおいて、ソフトウェア資産管理漏れ検出リストを作成することが可能となる。

すなわち、従来のソフトウェア資産管理システムを構成するサーバに対し、従来のソフトウェア資産管理システムの付加的機能として、上記構成を加えること

により、本発明におけるソフトウェア資産管理漏れ検出リストの作成を行わせるようにすることができる。

【0025】

本発明の請求項7記載のネットワークを利用したソフトウェア資産管理漏れ検出サーバは、請求項5記載のネットワークを利用したソフトウェア資産管理漏れ検出サーバが、ネットワーク接続コンピュータリスト及びソフトウェア資産管理リストにもとづいて、ソフトウェア資産管理リストに存在し、かつ、ネットワーク接続コンピュータリストに存在しないコンピュータを抽出し、非使用状態となっているコンピュータのリストを作成する構成としてある。

【0026】

また、本発明の請求項8記載のネットワークを利用したソフトウェア資産管理漏れ検出サーバは、請求項6記載のネットワークを利用したソフトウェア資産管理漏れ検出サーバにおいて、ソフトウェア資産管理漏れ検出部が、ネットワーク接続コンピュータリスト及びソフトウェア資産管理リストにもとづいて、ソフトウェア資産管理リストに存在し、かつ、ネットワーク接続コンピュータリストに存在しないコンピュータを抽出し、非使用状態となっているコンピュータのリストを作成する構成としてある。

【0027】

ネットワークを利用したソフトウェア資産管理漏れ検出サーバをこれらのような構成にすれば、以前使用されていたが、現在は使用されていないコンピュータを洗い出すことができる。

すなわち、ソフトウェア資産管理から漏れているコンピュータを検出することに加えて、現在未使用のソフトウェアの一覧を取得することも可能となる。

【0028】

本発明の請求項9記載のネットワークを利用したソフトウェア資産管理漏れ検出サーバは、請求項5～8のいずれかに記載のネットワークを利用したソフトウェア資産管理漏れ検出サーバが、ネットワーク接続コンピュータリスト及びソフトウェア資産管理リストをソートし、このソートしたネットワーク接続コンピュータリスト及びソフトウェア資産管理リストにもとづいて、ソフトウェア資産管

理漏れのコンピュータのリスト、又は、非使用状態となっているコンピュータのリストを作成する構成としてある。

【0029】

ネットワークを利用したソフトウェア資産管理漏れ検出サーバをこのような構成にすれば、例えば、ネットワーク接続コンピュータリスト及びソフトウェア資産管理リストのそれぞれを、ネットワークアドレスなどにもとづいて昇順、又は降順にソートすることによって、ソフトウェア資産管理漏れ検出リストの作成において、逐次探索アルゴリズムを利用する代わりに、二分探索アルゴリズムなどを利用した処理を行うことが可能となる。

このため、ソフトウェア資産管理漏れ検出リストや非使用コンピュータリストを生成する処理をより高速化することが可能となる。

【0030】

本発明の請求項10記載のネットワークを利用したソフトウェア資産管理漏れ検出プログラムは、コンピュータごとに、その基本情報及びインストールされているソフトウェア、修正パッチの適用状況を管理するソフトウェア資産管理から漏れているコンピュータを検出するためのネットワークを利用したソフトウェア資産管理漏れ検出プログラムであって、ソフトウェア資産管理漏れ検出サーバに、所定のネットワークに接続された全てのコンピュータについて、各コンピュータを特定するための情報を保有するネットワーク接続コンピュータリストを備えたネットワーク接続管理サーバから、ネットワーク接続コンピュータリストを受信させるとともに、ソフトウェア資産管理の管理対象となっている全てのコンピュータについて、各コンピュータを特定するための情報を保有するソフトウェア資産管理リストを備えたソフトウェア資産管理サーバから、ソフトウェア資産管理リストを受信させ、ネットワーク接続コンピュータリスト及びソフトウェア資産管理リストにもとづいて、ネットワーク接続コンピュータリストに存在し、かつ、ソフトウェア資産管理リストに存在しないコンピュータを抽出させ、ソフトウェア資産管理漏れのコンピュータのリストを作成させる構成としてある。

【0031】

ネットワークを利用したソフトウェア資産管理漏れ検出プログラムをこのよう

な構成にすれば、ソフトウェア資産管理漏れ検出サーバに、ネットワーク接続管理サーバからのネットワーク接続コンピュータリストと、ソフトウェア資産管理サーバからのソフトウェア資産管理リストにもとづいて、容易にソフトウェア資産管理漏れのコンピュータを検出させることが可能となる。

このため、OSやソフトウェアのバージョンやパッチ適用状態等も同時に管理するソフトウェア資産管理において、本発明のネットワークに接続されたコンピュータを漏れなく含んだリストを作成することにより、その管理漏れを防ぐことが可能となる。

#### 【0032】

本発明の請求項11記載のネットワークを利用したソフトウェア資産管理漏れ検出プログラムは、コンピュータごとに、その基本情報及びインストールされているソフトウェア、修正パッチの適用状況を管理するソフトウェア資産管理から漏れているコンピュータを検出するためのネットワークを利用したソフトウェア資産管理漏れ検出プログラムであって、ソフトウェア資産管理漏れ検出サーバに、所定のネットワークに接続された全てのコンピュータについて、各コンピュータを特定するための情報を保有するネットワーク接続コンピュータリストを作成させるとともに、ソフトウェア資産管理の管理対象となっている全てのコンピュータについて、各コンピュータを特定するための情報を保有するソフトウェア資産管理リストを作成させ、ネットワーク接続コンピュータリスト及びソフトウェア資産管理リストにもとづいて、ネットワーク接続コンピュータリストに存在し、かつ、ソフトウェア資産管理リストに存在しないコンピュータを抽出させ、ソフトウェア資産管理漏れのコンピュータのリストを作成させる構成としてある。

#### 【0033】

ネットワークを利用したソフトウェア資産管理漏れ検出プログラムをこのような構成にすれば、一台のソフトウェア資産管理漏れ検出サーバに、ソフトウェア資産管理漏れ検出リストを作成させることが可能となる。

そして、これによって、OSやソフトウェアのバージョンやパッチ適用状態等も同時に管理するソフトウェア資産管理において、その管理漏れを防ぐことが可能となる。

## 【0034】

本発明の請求項12記載のネットワークを利用したソフトウェア資産管理漏れ検出プログラムは、請求項10又は11記載のネットワークを利用したソフトウェア資産管理漏れ検出プログラムが、ソフトウェア資産管理漏れ検出サーバに、ネットワーク接続コンピュータリスト及びソフトウェア資産管理リストにもとづいて、ソフトウェア資産管理リストに存在し、かつ、ネットワーク接続コンピュータリストに存在しないコンピュータを抽出させ、非使用状態となっているコンピュータのリストを作成させる構成としてある。

## 【0035】

ネットワークを利用したソフトウェア資産管理漏れ検出プログラムをこのような構成にすれば、ソフトウェア資産管理漏れ検出サーバに、以前使用されていたが、現在は使用されていないコンピュータを洗い出させることができる。

また、これによって、ソフトウェア資産管理漏れ検出サーバに、現在未使用のソフトウェアの一覧を出力させることが可能となる。

## 【0036】

本発明の請求項13記載のネットワークを利用したソフトウェア資産管理漏れ検出プログラムは、請求項10～12のいずれかに記載のネットワークを利用したソフトウェア資産管理漏れ検出プログラムが、ソフトウェア資産管理漏れ検出サーバに、ネットワーク接続コンピュータリスト及びソフトウェア資産管理リストをソートさせ、このソートされたネットワーク接続コンピュータリスト及びソフトウェア資産管理リストにもとづいて、ソフトウェア資産管理漏れのコンピュータのリスト、又は、非使用状態となっているコンピュータのリストを作成させる構成としてある。

## 【0037】

ネットワークを利用したソフトウェア資産管理漏れ検出プログラムをこのような構成にすれば、ソフトウェア資産管理漏れ検出サーバに、ネットワーク接続コンピュータリスト及びソフトウェア資産管理リストをソートさせた後に、ソフトウェア資産管理漏れ検出リスト又は非使用コンピュータリストを作成させることが可能となる。

これによって、その作成処理を高速化させることが可能となる。

#### 【0038】

##### 【発明の実施の形態】

以下、本発明の実施形態につき、図面を参照して説明する。

##### [第一実施形態]

まず、本発明の第一実施形態について、図1及び図2を参照して説明する。図1は、本発明の第一実施形態のネットワークを利用したソフトウェア資産管理漏れ検出システムの構成を示すブロック図である。また、図2は、同システムにおけるネットワーク接続コンピュータリスト及びソフトウェア資産管理リストを示す図である。

図1に示すように、ネットワークを利用したソフトウェア資産管理漏れ検出システムは、ネットワーク接続管理サーバ10、ソフトウェア資産管理サーバ20、及びソフトウェア資産管理漏れ検出サーバ30により構成されている。

本実施形態においては、これらのサーバが、物理ネットワークとしてEthernet（登録商標）、ネットワークプロトコルとしてTCP/IP（Transmission Control Protocol/Internet Protocol）を用いて接続されているものとしているが、これに限定されるものではない。

#### 【0039】

ネットワーク接続管理サーバ10は、ネットワークに接続されているコンピュータを管理するサーバで、ネットワーク接続コンピュータリスト100を保有している。

このネットワーク接続コンピュータリスト100は、ネットワークに接続されているコンピュータを漏れなく含むようにリストアップできる手段であれば、どのような手段を用いて作成してもかまわない。

#### 【0040】

例えば、物理ネットワークにEthernet（登録商標）、ネットワークプロトコルにTCP/IPを用いる場合には、コンピュータがネットワークに接続して通信を行う際に、ARP（Address Resolution Pro

protocol) をブロードキャストして接続先コンピュータのMAC (Media Access Control) アドレスを特定する仕組みを利用することができる。

すなわち、各ブロードキャストドメインにパケットを監視する装置を設置してARPパケットを監視し、ARPパケットに含まれるMACアドレスとIPアドレスでコンピュータを検知してリストアップする。

そして、検知したIPアドレスを用いてDNS (Domain Name System) へ問い合わせ、コンピュータ名を特定することで、ネットワークに接続されたコンピュータを漏れなく含むネットワーク接続コンピュータリスト100を生成するという手段を用いることができる。

#### 【0041】

ソフトウェア資産管理サーバ20は、組織内で購入利用されているソフトウェア資産の利用状況を管理するサーバであり、ソフトウェア資産管理リスト200を保有している。

このソフトウェア資産管理リスト200は、各コンピュータにインストールされているOS (Operating System) やアプリケーションの種類や名前、パッチ適用状態などのソフトウェア資産管理情報と、MACアドレスやIPアドレス、コンピュータ名などのコンピュータの基本情報をリストアップできる手段であれば、どのような手段を用いて作成してもかまわない。

#### 【0042】

例えば、各コンピュータにおいて、ソフトウェア資産管理情報とコンピュータの基本情報を調査するエージェントソフトを動作させ、調査結果をソフトウェア資産管理サーバ200に送信させる。

そして、この各コンピュータから送信されてきた情報にもとづいて、ソフトウェア資産管理サーバ20に、ソフトウェア資産管理リスト200を生成させるという手段を用いることができる。

#### 【0043】

ソフトウェア資産管理漏れ検出サーバ30は、ネットワーク接続管理サーバ10からネットワーク接続コンピュータリスト100を受信するとともに、ソフト

ウェア資産管理サーバ20からソフトウェア資産管理リスト200を受信する。

そして、Ethernet（登録商標）での通信でコンピュータを識別するために利用するMACアドレスをキーとして、ネットワーク接続コンピュータリスト100とソフトウェア資産管理リスト200とを比較し、ソフトウェア資産管理リスト200から漏れているコンピュータの洗い出しを行う。

#### 【0044】

このコンピュータの洗い出しについて、図2を用いて説明する。同図において、ネットワーク接続コンピュータリスト100は、ネットワークに接続されたコンピュータを漏れなく検出する手段を用いて生成されたものであり、ネットワークアドレス111～11m、及びこれに対応するコンピュータ名121～12mを有している。

また、ソフトウェア資産管理情報リスト200は、各コンピュータ単位でコンピュータの基本情報やインストールされているOS、アプリケーションソフト等を整理分類したものである。ここでは、基本情報として、ネットワークアドレスとコンピュータ名が登録されている。

#### 【0045】

コンピュータの洗い出しにあたっては、ネットワーク接続コンピュータリスト100におけるネットワークアドレス111～11mと、ソフトウェア資産管理情報リスト200におけるネットワークアドレス211～21nを比較し、111～11mに含まれており211～21nに含まれていないアドレスを持つコンピュータはソフトウェア資産管理情報から漏れているコンピュータと判断する。

この方法により、ネットワークに接続されているコンピュータで利用されているソフトウェア資産の管理漏れを防止することが容易となり、またOSやアプリケーションのパッチ適用状態が不明なコンピュータがネットワークに接続されたままとなりセキュリティ上問題となる状況を防止することが容易となる。

#### 【0046】

次に、本実施形態のネットワークを利用したソフトウェア資産管理漏れ検出サーバ30における処理手順につき、図3を参照して説明する。同図は、本実施形態のネットワークを利用したソフトウェア資産管理漏れ検出システムにおける処



理手順を示すフローチャートである。

まず、同フローチャートにおける処理に先立ち、ソフトウェア資産管理漏れ検出サーバ30は、ネットワーク接続管理サーバ10からネットワーク接続コンピュータリスト100を、ソフトウェア資産管理サーバ20からソフトウェア資産管理リスト200を受信する。

そして、ソフトウェア資産管理漏れ検出サーバ30は、これらのリストにもとづいて、以下に示すように、ソフトウェア資産管理情報から漏れているコンピュータの洗い出しを行う。なお、図3のフローチャートにおける動作の主体は、ソフトウェア資産管理漏れ検出サーバ30であるが、以下の説明においては、その記載を省略する。

#### 【0047】

まず、ネットワーク接続コンピュータリスト100の先頭に記述されているコンピュータのMACアドレス情報を取り出す（ステップA1）。引き続きステップA2～A6までの動作は、この取り出したMACアドレス11iを持つコンピュータが、ソフトウェア資産管理リスト200に含まれているかどうかを判断し、含まれていない場合はソフトウェア資産管理漏れコンピュータリスト300に追加するという動作を表している。

#### 【0048】

すなわち、ソフトウェア資産管理リスト200の先頭に記述されているコンピュータのMACアドレス情報を取り出す（ステップA2）。

そして、ステップA1で取り出したMACアドレスとステップA2で取り出したMACアドレスの比較を行い（ステップA3）、両者が同じであれば、接続コンピュータリスト100から取り出したMACアドレス11iに該当するコンピュータが、ソフトウェア資産管理リスト200に含まれていると判断し、ステップA7へ進む。

#### 【0049】

また、MACアドレスが異なる場合は、ステップA3における比較で用いたMACアドレスのうち、ソフトウェア資産管理リスト200から取り出したMACアドレス21jが、ソフトウェア資産管理リスト200の最後のコンピュータの

MACアドレスであるかどうかを判断する（ステップA4）。

そして、MACアドレス21jが、リストの最後のコンピュータのMACアドレスでなければ、リスト200の次のコンピュータのMACアドレスを取り出して（ステップA5）、再びステップA3からの処理を実行する。

#### 【0050】

MACアドレス21jが、資産管理リスト200の最後のコンピュータのMACアドレスであれば、ネットワーク接続コンピュータリスト100から取り出したMACアドレス11iに該当するコンピュータが、ソフトウェア資産管理リスト200に含まれていないと判断し、ステップA6に進む。

そして、MACアドレス11iのコンピュータの情報をネットワーク接続コンピュータリスト100から取り出し、ソフトウェア資産管理漏れコンピュータリスト300へ追加して（ステップA6）、ステップA7に進む。

#### 【0051】

そして、MACアドレス11iが、ネットワーク接続コンピュータリスト100の最後のコンピュータのMACアドレスであるかどうかを判断し（ステップA7）、MACアドレス11iが、リスト100の最後のコンピュータのMACアドレスでなければ、次のコンピュータリストのMACアドレスを取り出して（ステップA8）、ステップA2～A6の処理を繰り返す。

MACアドレス11iが、リスト100の最後のコンピュータのMACアドレスの場合は、このネットワーク接続コンピュータリスト100に含まれるすべてのコンピュータに対して、ソフトウェア資産管理リスト200に含まれているかどうかを判断したことになるため、処理を終了する。

#### 【0052】

次に、図4及び図5を用いて、本実施形態のネットワークを利用したソフトウェア資源管理漏れ検出システムの処理手順について、具体例を用いて説明する。

図4は、本実施形態のネットワークを利用したソフトウェア資源管理漏れ検出システムにおけるネットワーク接続コンピュータリスト及びソフトウェア資産管理リストの具体例を示す図である。図5は、同システムにおけるソフトウェア資産管理漏れのコンピュータのリスト、すなわちソフトウェア資産管理漏れ検出リ

ストの具体例を示す図である。

以下に、図4に示すネットワーク接続コンピュータリスト100、及びソフトウェア資産管理リスト200を用いて、図3に示す上述の処理手順を実行した場合につき、具体的に説明する。

#### 【0053】

まず、ステップA1において、ネットワーク接続コンピュータリスト100からリストの先頭のMACアドレス「00:00:4c:11:11:11」を取り出す。

そしてステップA2において、ソフトウェア資産管理リスト200からリストの先頭のMACアドレス「00:00:4c:55:55:55」を取り出す。

#### 【0054】

次に、ステップA3で、取り出したMACアドレスの比較を行う。この場合、それぞれのリストから取り出したMACアドレスが異なっているため、ステップA4に進む。

ステップA4では、ソフトウェア資産管理リスト200から取り出したMACアドレスがリストの最後のものを判断する。この場合は、リストの最後ではないので、ステップA5に進み、リストの次のMACアドレス「00:00:4c:11:11:11」を取り出してステップA3に戻る。

#### 【0055】

次のステップA3でのMACアドレスの比較では、MACアドレスが一致しているため、ステップA7に進む。

ステップA7では、ネットワーク接続コンピュータリストから取り出したMACアドレスが、リスト100の最後のものを判断する。この場合はリスト100の最後のものではないため、ステップA8に進み、リスト100の次のMACアドレス「00:00:4c:22:22:22」を取り出してステップA2に戻る。

#### 【0056】

これ以降の動作は、ネットワーク接続コンピュータリスト100から取り出しMACアドレスが「00:00:4c:11:11:11」の場合と同様である

しかし、MACアドレス「00:00:4c:22:22:22」のコンピュータは、ソフトウェア資産管理リスト200に登録されていない。

このため、ソフトウェア資産管理リスト200の最後のコンピュータである「00:00:4c:77:77:77」のMACアドレスが処理される場合は、ステップA4から、ステップA6に処理が進む。そして、ソフトウェア資産管理漏れリスト300に、MACアドレスが「00:00:4c:22:22:22」のコンピュータの情報が追加される。

#### 【0057】

同様に、ネットワーク接続コンピュータリストに登録されているコンピュータのうち、MACアドレスが「00:00:4c:55:55:55」、「00:00:4c:77:77:77」のコンピュータに関しては、ソフトウェア資産管理リスト200にも登録されている。

このため、これらのコンピュータについては、MACアドレスが、「00:00:4c:11:11:11」のコンピュータの時と同様の動作となる。

#### 【0058】

また、MACアドレスが「00:00:4c:bb:bb:bb」のコンピュータに関しては、ソフトウェア資産管理リスト200に登録されていないため、MACアドレスが「00:00:4c:22:22:22」のコンピュータの時と同様の動作となる。

ただし、このMACアドレスが「00:00:4c:bb:bb:bb」のコンピュータは、ネットワーク接続コンピュータリスト100の最後のMACアドレスであるため、ステップA7の処理後、終了する。

以上の処理によって、図5に示すソフトウェア資産管理漏れリスト300が作成される。

#### 【0059】

以上説明したように、本実施形態のネットワークを利用したソフトウェア資産管理漏れ検出システムによれば、ソフトウェア資産管理から漏れているコンピュータを容易に洗い出すことが可能となる。

また、従来のソフトウェア資産管理システムを大幅に変更することなくソフトウェア資産管理情報の漏れを防止することが可能となる。

その結果、OSやソフトウェアのバージョンやパッチ適用状態等が不明なコンピュータを検出し、パッチ適用状態が最新ではなくセキュリティホールとなりうるコンピュータがネットワークに接続されたままになることを防止することが可能となる。

さらに、ネットワーク接続コンピュータリストとソフトウェア資産管理リストを適切な間隔で定期的に更新して比較することにより、ソフトウェア資産管理外のコンピュータや不正なコンピュータが接続された場合に、これを早期に発見することが可能となる。

#### 【0060】

##### [第二実施形態]

次に、本発明の第二実施形態について、図3、及び図6～図8を参照して説明する。図6は、本実施形態のネットワークを利用したソフトウェア資産管理漏れ検出システムにおける処理手順を示すフローチャートである。図7は、同システムにおけるネットワーク接続コンピュータリスト及びソフトウェア資産管理リストの具体例を示す図である。図8は、同システムにおけるソフトウェア資産管理漏れ検出リストと、非使用状態となっているコンピュータのリスト、すなわち非使用コンピュータリストの具体例を示す図である。

本実施形態は、以前使用されていたが、現在は使用されていないコンピュータを洗い出すことができる点で第一実施形態と異なる。

#### 【0061】

図6のフローチャートにおける動作手順は、図3のフローチャートにおけるネットワーク接続コンピュータリスト100とソフトウェア資産管理リスト200との関係を逆転させたものである。

これによって、ソフトウェア資産管理リストに含まれているが、ネットワーク接続コンピュータリストには含まれていないコンピュータを検出することが可能となり、これを既にご利用されていないコンピュータと判断することができる。

また、ソフトウェア資産管理漏れ検出サーバ30に、図3のフローチャートの

処理終了後に図6のフローチャートの処理を行わせることによって、ソフトウェア資産管理漏れコンピュータリスト300、及び非使用コンピュータリスト400を共に生成することができる。

すなわち、ソフトウェア資産管理から漏れているコンピュータを検出するとともに、現在未使用のソフトウェアの一覧を取得することが可能となり、ソフトウェア資産管理をより厳密に行うことが容易となる。

#### 【0062】

次に、図7に示すネットワーク接続リスト100、及びソフトウェア資産管理リスト200を用いて、図3のフローチャートと図6のフローチャートを連続して処理する場合の動作について、具体的に説明する。

図7のリストは、図4のリストのうち、ソフトウェア資産管理リスト200に、ネットワーク接続コンピュータリスト100に含まれていない2台分のコンピュータの情報を追加したものであり、ネットワーク接続コンピュータリスト100は図4のものと同一である。

つまり、図7のリストにおいて、ネットワーク接続コンピュータリスト100に含まれており、ソフトウェア資産管理リスト200に含まれていないコンピュータは図4のリストと同様となる。

したがって、図7のリストを用いた場合に、ソフトウェア資産管理漏れリスト300に追加されるコンピュータは、図4のリストを用いた場合と同じになるため、図3のフローチャートによるソフトウェア資産管理漏れリスト300を生成する処理の詳細な動作の説明は省略する。

#### 【0063】

続いて、図3のフローチャートの処理後に実行される、図6のフローチャートの処理について詳細に説明する。

まず、ソフトウェア資産管理リスト200からリストの先頭のMACアドレス「00:00:4c:55:55:55」を取り出し（ステップB1）、ネットワーク接続コンピュータリスト100からリストの先頭のMACアドレス「00:00:4c:11:11:11」を取り出す（ステップB2）。

次に、取り出したMACアドレスの比較を行う（ステップB3）。この場合、

それぞれのリストから取り出したMACアドレスが異なっているため、ステップB4に進む。

#### 【0064】

そして、ネットワーク接続コンピュータリスト100から取り出したMACアドレスがリスト100の最後のものかを判断する（ステップB4）。この場合はリストの最後ではないので、リストの次のMACアドレス「00:00:4c:22:22:22」を取り出して（ステップB5）、ステップB3に戻る。

次のステップB3でのMACアドレスの比較も同様にMACアドレスが異なっているため、ステップB4、ステップB5の順番に処理が進み、ネットワーク接続コンピュータリスト100の次のMACアドレス「00:00:4c:55:55:55」を取り出してステップB3に戻る。

#### 【0065】

次のステップB3でのMACアドレスの比較では、MACアドレスが一致しているため、ステップB7に進む。

そして、ソフトウェア資産管理リスト200から取り出したMACアドレスがリスト200の最後のものかを判断する（ステップB7）。この場合はリスト200の最後のものではないため、ステップB8に進む。

そして、リストの次のMACアドレス「00:00:4c:33:33:33」を取り出して（ステップB8）、ステップB2に戻る。

#### 【0066】

これ以降の動作は、ソフトウェア資産管理リスト200から取り出したMACアドレスが「00:00:4c:55:55:55」の場合と同様であるが、ネットワーク接続コンピュータリスト100にはMACアドレス「00:00:4c:33:33:33」のコンピュータが登録されていない。

このため、ネットワーク接続コンピュータリスト100から取り出したMACアドレスが「00:00:4c:bb:bb:bb」の時、ステップB4において、これはネットワーク接続コンピュータリスト100の最後のMACアドレスのため、ステップB6に進み、非使用コンピュータリスト400に、MACアドレスが「00:00:4c:33:33:33」のコンピュータの情報が追加さ

れる (ステップB6)。

#### 【0067】

ソフトウェア資産管理リスト200に登録されているコンピュータのうち、MACアドレスが「00:00:4c:11:11:11」、「00:00:4c:77:77:77」のコンピュータに関しては、ネットワーク接続コンピュータリスト100にも登録されているため、MACアドレスが、「00:00:4c:55:55:55」のコンピュータの時と同様の動作となる。

また、MACアドレスが「00:00:4c:88:88:88」のコンピュータに関しては、ネットワーク接続コンピュータリスト100に登録されていないため、MACアドレスが「00:00:4c:33:33:33」のコンピュータの時と同様の動作となる。

#### 【0068】

そして、リスト200におけるMACアドレスが「00:00:4c:77:77:77」のコンピュータについては、ソフトウェア資産管理リスト200の最後のMACアドレスであるため、ステップB7の処理後、終了する。

図8は、このようにして生成されたソフトウェア資産管理漏れリスト300、及び非使用コンピュータリスト400を示している。

#### 【0069】

以上説明したように、本実施形態のネットワークを利用したソフトウェア資産管理漏れ検出システムによれば、ソフトウェア資産管理漏れリストのみならず、非使用コンピュータリストを生成することができ、すでに使用されていないコンピュータを洗い出すことが可能となる。

すなわち、ソフトウェア資産管理から漏れているコンピュータを検出するとともに、現在未使用のソフトウェアの一覧を取得することが可能となり、ソフトウェア資産管理をより厳密に行うことが容易となる。

#### 【0070】

#### [第三実施形態]

次に、本発明の第三実施形態について、図9を参照して説明する。同図は、本実施形態のネットワークを利用したソフトウェア資産管理漏れ検出サーバの構成



を示すブロック図である。

本実施形態は、ソフトウェア資産管理漏れ検出リスト300や非使用コンピュータリスト400の作成を、一台のサーバにより行うことができる点で第一、及び第二実施形態と異なる。

#### 【0071】

すなわち、図9において、資産統合管理サーバ1000は、図1におけるネットワーク接続管理サーバ10、ソフトウェア資産管理サーバ20、ソフトウェア資産管理漏れ検出サーバ30の3つのサーバに分かれている構成を、一つのサーバにまとめたものである。

図9において、ネットワーク接続管理部1010が図1のネットワーク接続管理サーバ10の機能を、ソフトウェア資産管理部1020がソフトウェア資産管理サーバ20の機能を、そしてソフトウェア資産管理漏れ検出部1030がソフトウェア資産管理漏れ検出サーバ30の機能を実現している。

このように、本発明を実施する際には、各機能毎にサーバを設置してもよく、また各機能を1台のサーバで実現してもよい。

#### 【0072】

##### [第四実施形態]

次に、本発明の四実施形態について、図10を参照して説明する。同図は、本実施形態のネットワークを利用したソフトウェア資産管理漏れ検出サーバの構成を示すブロック図である。

本実施形態は、ソフトウェア資産管理漏れリスト300又は未使用コンピュータリスト400の作成にあたり、ネットワーク接続コンピュータリスト100及びソフトウェア資産管理リスト200をそれぞれソートした後に用いる点で第三実施形態と異なる。

#### 【0073】

すなわち、図10において、資産統合管理サーバ1000は、第三実施形態における構成に加えてリスト前処理部1040を有している。

このリスト前処理部1040において、ネットワーク接続コンピュータリスト100とソフトウェア資産管理情報リスト200をそれぞれMACアドレスに対

して昇順、又は降順にソートすることにより、ソフトウェア資産管理漏れ検出部 1030では逐次探索アルゴリズムを利用する処理の代わりに、例えば二分探索アルゴリズムを利用した処理を行うことが可能となる。

その結果、ソフトウェア資産管理漏れリスト300と未使用コンピュータリスト400を生成する処理を高速化することが可能となる。

#### 【0074】

このように、本発明を実施する際には、図1におけるネットワークアドレスをキーとしたリスト比較処理が可能なアルゴリズムであれば、どのようなアルゴリズムを用いてもよい。

また、このようなリスト前処理を、第一実施形態又は第二実施形態において、行うようにすることももちろん可能である。

このとき、リスト前処理を、ネットワーク接続管理サーバ10において、ネットワーク接続コンピュータリスト100に対して行うとともに、ソフトウェア資産管理サーバ20において、ソフトウェア資産管理リスト200に対して行うようにすることができる。

また、リスト前処理をソフトウェア資産管理漏れ検出サーバ30において、ネットワーク接続コンピュータリスト100及びソフトウェア資産管理リスト200の双方に対して行うようにしてもよい。

#### 【0075】

上記の実施形態におけるソフトウェア資産管理漏れの検出や、ソフトウェア資産管理漏れ検出リストの作成等は、ネットワークを利用したソフトウェア資産管理漏れ検出プログラムにより実行される。

このネットワークを利用したソフトウェア資産管理漏れ検出プログラムは、コンピュータの各構成要素に指令を送り、所定の処理、例えば、ソフトウェア資産管理漏れの検出処理や、ソフトウェア資産管理漏れ検出リストの作成処理等を行わせる。

これによって、これらの処理は、ネットワークを利用したソフトウェア資産管理漏れ検出プログラムとコンピュータとが協働したネットワークを利用したソフトウェア資産管理漏れ検出サーバ30などにより実現される。

## 【0076】

なお、ネットワークを利用したソフトウェア資産管理漏れ検出プログラムは、コンピュータのROMやハードディスクに記憶させる他、コンピュータ読み取り可能な記録媒体、たとえば、外部記憶装置及び可搬記録媒体等に格納することができる。

外部記憶装置とは、磁気ディスク等の記録媒体を内蔵し、例えばネットワークを利用したソフトウェア資産管理漏れ検出サーバ30などに外部接続される記憶増設装置をいう。一方、可搬記録媒体とは、記録媒体駆動装置（ドライブ装置）に装着でき、かつ、持ち運び可能な記録媒体であって、たとえば、CD-ROM、フレキシブルディスク、メモリカード、光磁気ディスク等をいう。

## 【0077】

そして、記録媒体に記録されたプログラムは、コンピュータのRAMにロードされて、CPUにより実行される。この実行により、上述した本実施形態のネットワークを利用したソフトウェア資産管理漏れ検出サーバ30の手段が実現される。

さらに、コンピュータでネットワークを利用したソフトウェア資産管理漏れ検出プログラムをロードする場合、他のコンピュータで保有されたネットワークを利用したソフトウェア資産管理漏れ検出プログラムを、通信回線を利用して自己の有するRAMや外部記憶装置にダウンロードすることもできる。

このダウンロードされたネットワークを利用したソフトウェア資産管理漏れ検出プログラムも、CPUにより実行され、本実施形態のソフトウェア資産管理漏れの検出処理や、ソフトウェア資産管理漏れ検出リストの作成処理等を実現する。

## 【0078】

なお、本発明は以上の実施形態に限定されるものではなく、本発明の範囲内において、種々の変更実施が可能であることは言うまでもない。

例えば、ネットワーク接続コンピュータリスト100及びソフトウェア資産管理リスト200を比較する際のキーとして、MACアドレス以外のネットワークアドレスやコンピュータを一意に識別可能な他のキーを利用するなど適宜設計変

更することのできるものである。

【0079】

【発明の効果】

以上のように、本発明によれば、ソフトウェア資産管理情報とは別にネットワークに接続されているコンピュータを漏れなく含むリストを作成し、ネットワークアドレスなどネットワーク上でコンピュータを一意に識別することが可能な情報を用いることで、ソフトウェア資産管理から漏れているコンピュータを見つけ出すことができる。

このため、ソフトウェア資産管理から漏れているコンピュータを容易に洗い出すことが可能となる。

【0080】

また、ネットワークに接続されているコンピュータを漏れなく含むリストを作成する手段を、従来のソフトウェア資産管理システムから独立して構成し、ソフトウェア資産管理漏れのコンピュータを検出することができる。

そして、このソフトウェア資産管理漏れのコンピュータに対して、従来のソフトウェア資産管理システムを適用することが可能となる。

このため、従来のソフトウェア資産管理システムを大幅に変更することなくソフトウェア資産管理情報の漏れを防止することが可能となる。

【0081】

その結果、OSやソフトウェアのバージョンやパッチ適用状態等も同時に管理するソフトウェア資産管理において、ネットワークに接続されたコンピュータを漏れなく含んだリストを用いることによって、管理漏れを防ぐことが可能となる。

このため、OSやソフトウェアのバージョンやパッチ適用状態等が不明なコンピュータを検出し、パッチ適用状態が最新ではなくセキュリティホールとなりうるコンピュータがネットワークに接続されたままになることを防止することが可能となる。

【0082】

また、ネットワーク接続コンピュータリストとソフトウェア資産管理リストを

1 日ごとなど適切な間隔で定期的に更新して比較することにより、新規にネットワークに接続されたコンピュータがソフトウェア資産管理下にあるかどうかを確認することができる。

このため、ソフトウェア資産管理外のコンピュータや不正なコンピュータが接続された場合、管理外コンピュータとして早期に発見することが可能となる。

#### 【0083】

さらに、ソフトウェア資産管理漏れリストのみならず、非使用コンピュータリストを生成することができ、すでに使用されていないコンピュータを洗い出すことが可能となる。

すなわち、ソフトウェア資産管理から漏れているコンピュータを検出するとともに、現在未使用のソフトウェアの一覧を取得することが可能となり、ソフトウェア資産管理をより厳密に行うことが容易となる。

#### 【0084】

加えて、ネットワークを利用したソフトウェア資産管理漏れ検出プログラムは、ネットワークを利用したソフトウェア資産管理漏れ検出サーバの制御部へ所定の指令を送ることにより、このソフトウェア資産管理漏れの検出機能や、ソフトウェア資産管理漏れ検出リストの作成機能等を実現させることができる。

これによって、これらの機能等は、ネットワークを利用したソフトウェア資産管理漏れ検出プログラムとネットワークを利用したソフトウェア資産管理漏れ検出サーバとが協働して実現することが可能である。

#### 【図面の簡単な説明】

##### 【図1】

本発明の第一実施形態のネットワークを利用したソフトウェア資産管理漏れ検出システムの構成を示すブロック図である。

##### 【図2】

本発明の第一実施形態のネットワークを利用したソフトウェア資産管理漏れ検出システムにおけるネットワーク接続コンピュータリスト及びソフトウェア資産管理リストを示す図である。

##### 【図3】

本発明の第一実施形態のネットワークを利用したソフトウェア資産管理漏れ検出システムにおける処理手順を示すフローチャートである。

【図4】

本発明の第一実施形態のネットワークを利用したソフトウェア資産管理漏れ検出システムにおけるネットワーク接続コンピュータリスト及びソフトウェア資産管理リストの具体例を示す図である。

【図5】

本発明の第一実施形態のネットワークを利用したソフトウェア資産管理漏れ検出システムにおけるソフトウェア資産管理漏れリストの具体例を示す図である。

【図6】

本発明の第二実施形態のネットワークを利用したソフトウェア資産管理漏れ検出システムにおける処理手順を示すフローチャートである。

【図7】

本発明の第二実施形態のネットワークを利用したソフトウェア資産管理漏れ検出システムにおけるネットワーク接続コンピュータリスト及びソフトウェア資産管理リストの具体例を示す図である。

【図8】

本発明の第二実施形態のネットワークを利用したソフトウェア資産管理漏れ検出システムにおけるソフトウェア資産管理漏れリスト及び非使用コンピュータリストの具体例を示す図である。

【図9】

本発明の第三実施形態のネットワークを利用したソフトウェア資産管理漏れ検出サーバの構成を示すブロック図である。

【図10】

本発明の第四実施形態のネットワークを利用したソフトウェア資産管理漏れ検出サーバの構成を示すブロック図である。

【符号の説明】

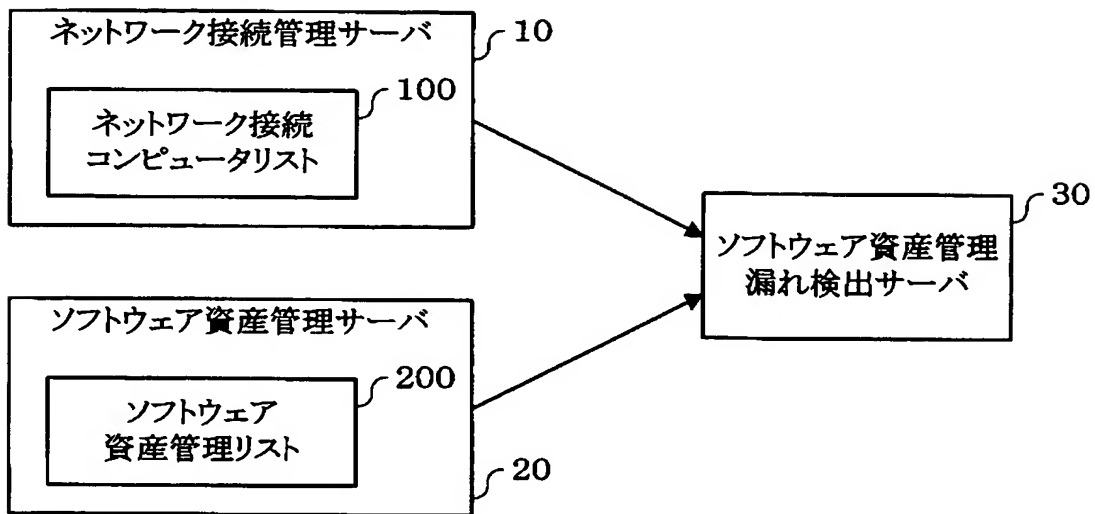
10 ネットワーク接続管理サーバ

100 ネットワーク接続コンピュータリスト

2 0 ソフトウェア資産管理サーバ  
2 0 0 ソフトウェア資産管理リスト  
3 0 ソフトウェア資産管理漏れ検出サーバ  
3 0 0 ソフトウェア資産管理漏れリスト  
4 0 0 非使用コンピュータリスト  
1 0 0 0 資産統合管理サーバ  
1 0 1 0 ネットワーク接続管理部  
1 0 2 0 ソフトウェア資産管理部  
1 0 3 0 ソフトウェア資産管理漏れ検出部  
1 0 4 0 リスト前処理部

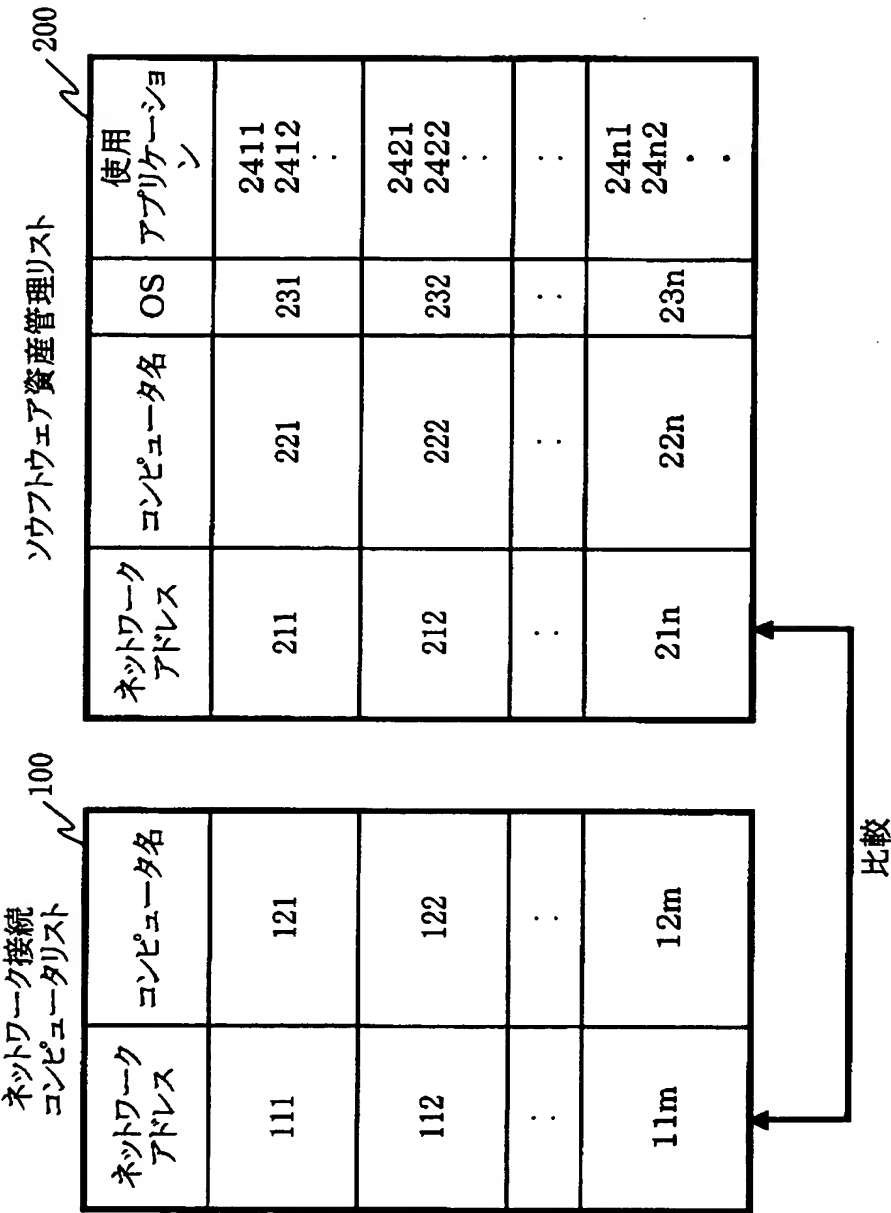
【書類名】 図面

【図 1】

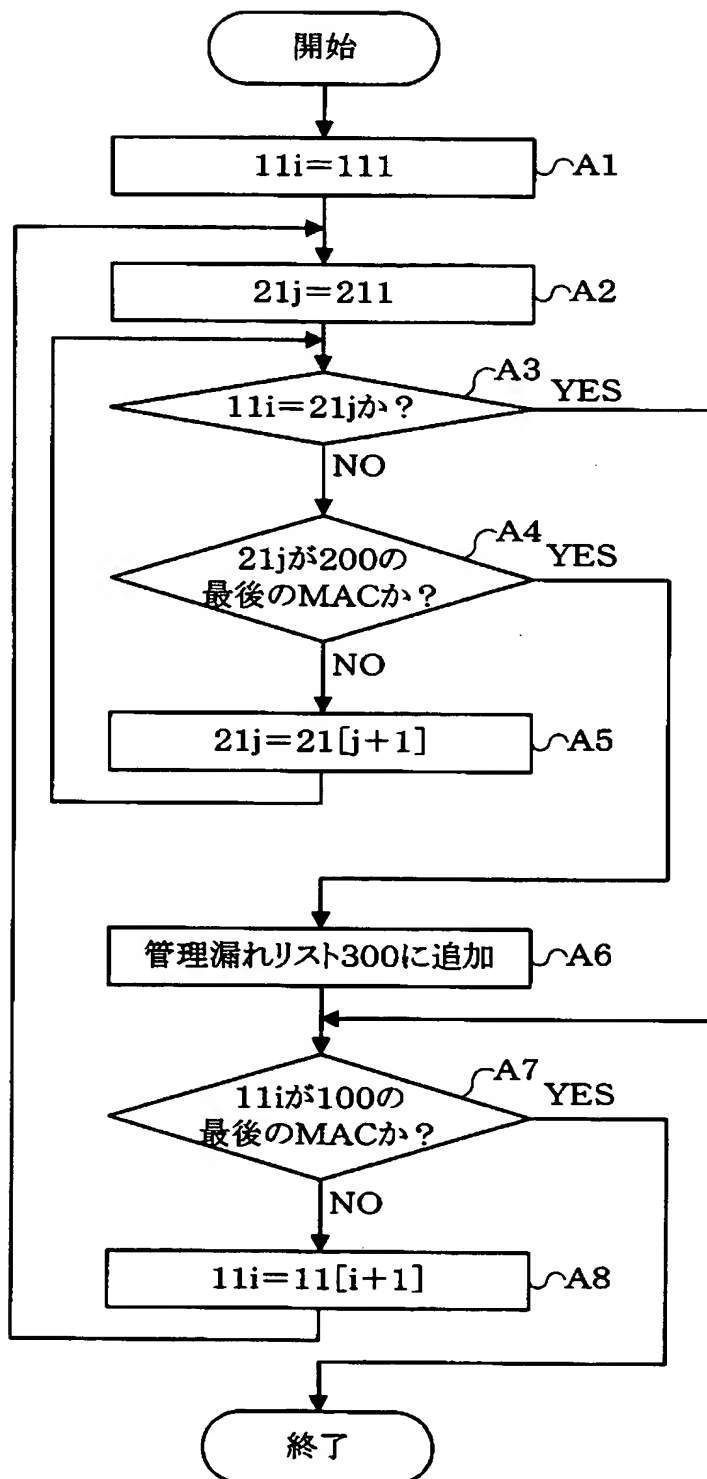




【図 2】



【図3】



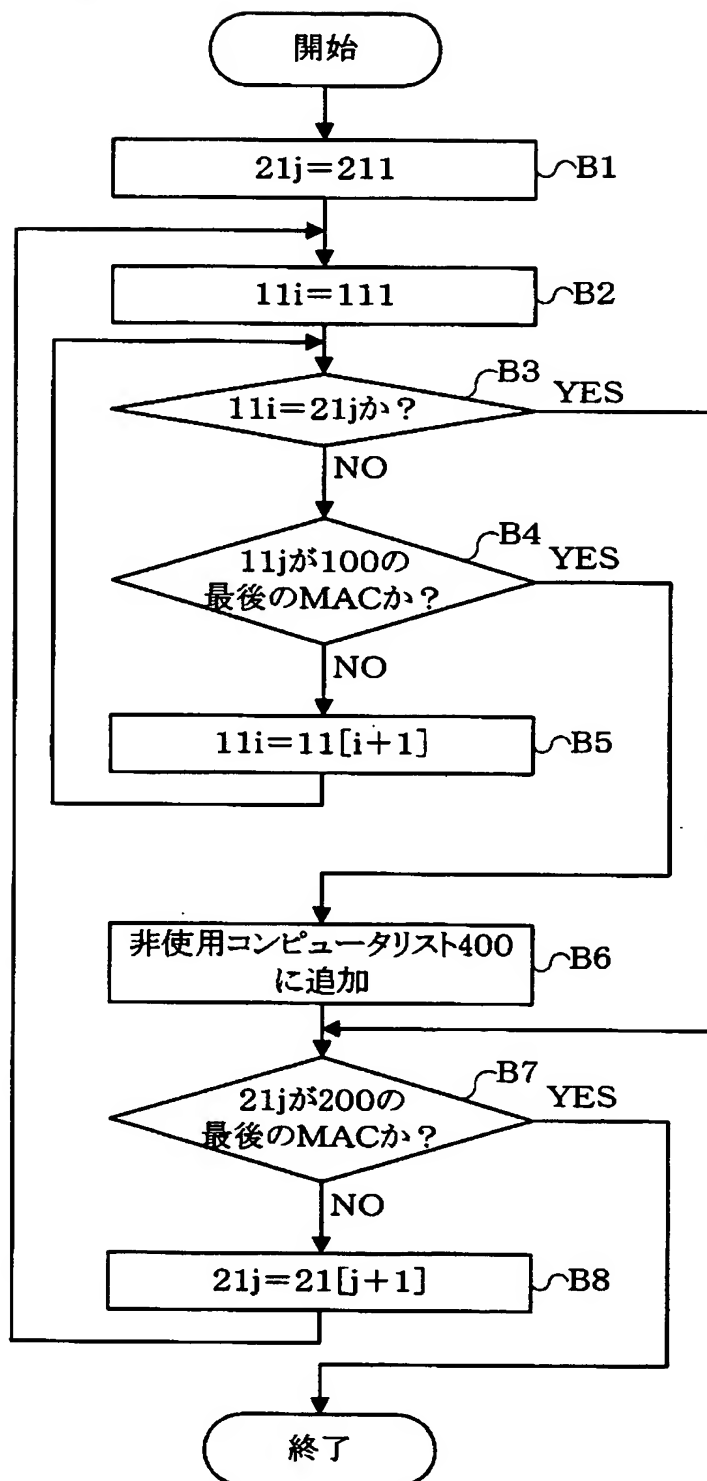
【図 4】

ネットワーク接続コンピュータリスト			ソフトウェア資産管理リスト			
MACアドレス	IPアドレス	コンピュータ名	MACアドレス	IPアドレス	コンピュータ名	利用アプリケーション
00:00:4c:11:11:11	192.168.0.1	host1	00:00:4c:55:55:55	192.168.0.100	host100	App1, App2
00:00:4c:22:22:22	192.168.0.4	host2	00:00:4c:11:11:11	192.168.0.1	host1	App1, App3, App4
00:00:4c:55:55:55	192.168.0.100	host100	00:00:4c:77:77:77	192.168.1.50	host50	App1, App2, App3
00:00:4c:77:77:77	192.168.1.50	host50				
00:00:4c:bb:bb:bb	102.168.5.3	host3				

【図 5】

ソフトウェア資産管理漏れリスト		
MACアドレス	IPアドレス	コンピュータ名
00:00:4c:22:22:22	192.168.0.4	host2
00:00:4c:bb:bb:bb	102.168.5.3	host3

【図 6】



【図 7】.

ネットワーク接続コンピュータリスト

MACアドレス	IPアドレス	コンピュータ名
00:00:4c:11:11:11	192.168.0.1	host1
00:00:4c:22:22:22	192.168.0.4	host2
00:00:4c:55:55:55	192.168.0.100	host100
00:00:4c:77:77:77	192.168.1.50	host50
00:00:4c:bb:bb:bb	102.168.5.3	host3

ソフトウェア資産管理リスト

MACアドレス	IPアドレス	コンピュータ名	OS	利用アプリケーション
00:00:4c:55:55:55	192.168.0.100	host100	OS1	App1,App2
00:00:4c:33:33:33	192.168.0.3	host3	OS1	App1,App2,App4
00:00:4c:11:11:11	192.168.0.1	host1	OS1	App1,App3,App4
00:00:4c:88:88:88	192.168.5.20	host20	OS2	App1,App4
00:00:4c:77:77:77	192.168.1.50	host50	OS2	App1,App2,App3

【図 8】

ソフトウェア資産管理漏れリスト

〜 300

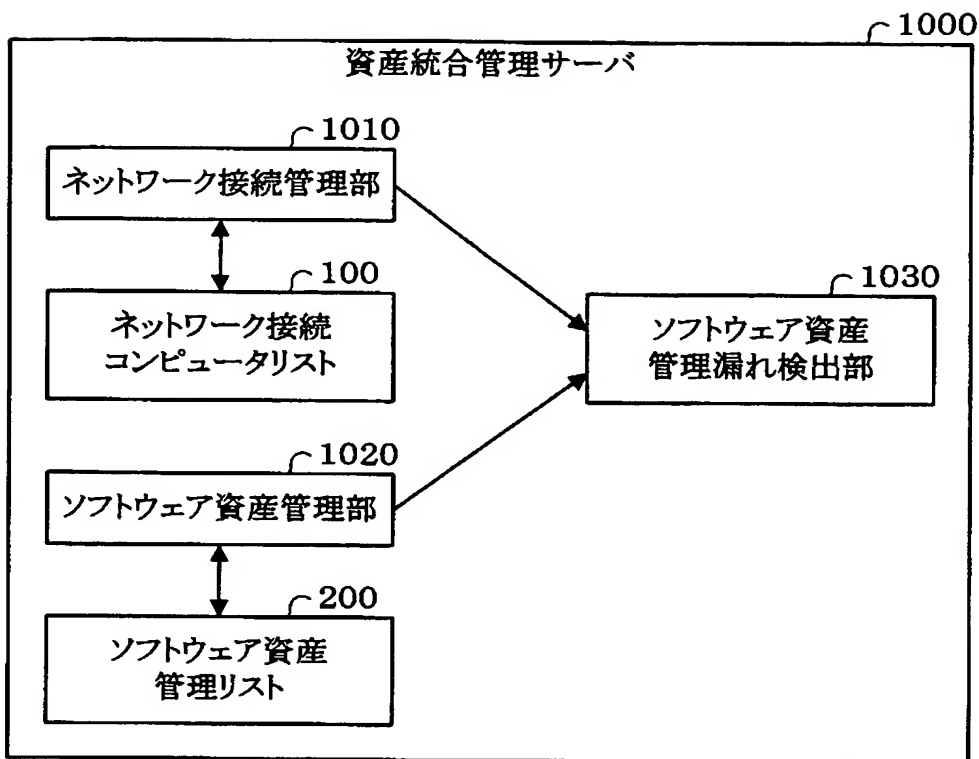
MACアドレス	IPアドレス	コンピュータ名
00:00:4c:22:22:22	192.168.0.4	host2
00:00:4c:bb:bb:bb	102.168.5.3	host3

非使用コンピュータリスト

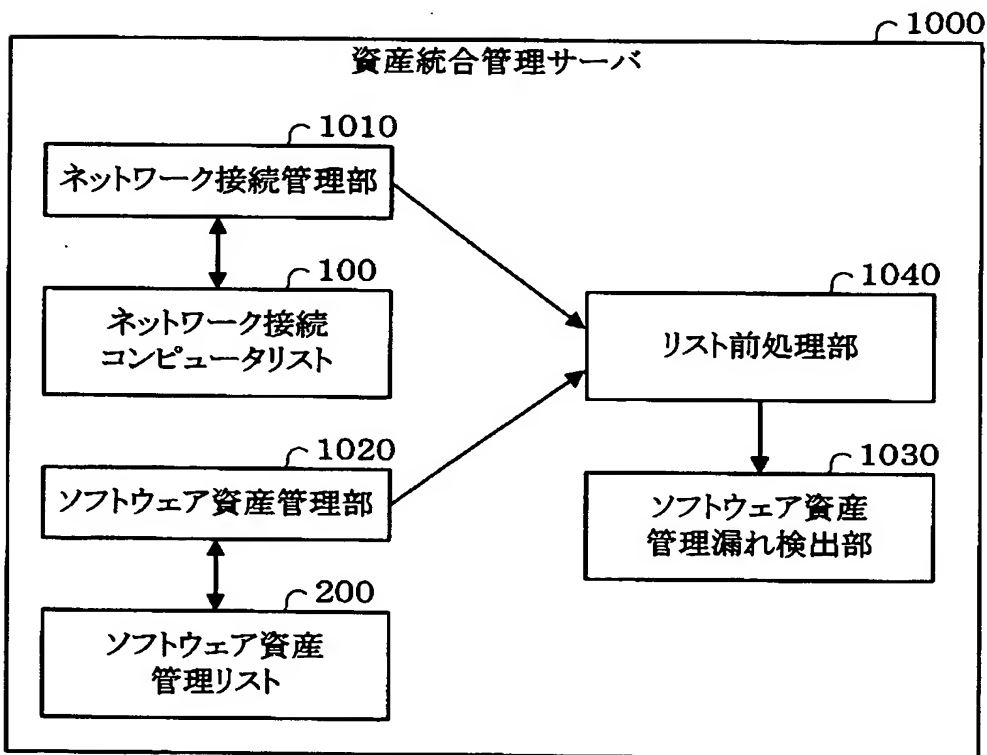
〜 400

MACアドレス	IPアドレス	コンピュータ名	OS	利用アプリケーション
00:00:4c:33:33:33	192.168.0.3	host3	OS1	App1,App2,App4
00:00:4c:88:88:88	192.168.5.20	host20	OS2	App1,App4

【図 9】



【図 10】



【書類名】 要約書

【要約】

【課題】 コンピュータごとに、その基本情報及びインストールされているソフトウェア、修正パッチの適用状況を管理するソフトウェア資産管理から、管理すべきコンピュータが漏れることを防止する。

【解決手段】 所定のネットワークに接続された全てのコンピュータについて、各コンピュータを特定するための情報を保有するネットワーク接続コンピュータリスト100と、ソフトウェア資産管理の管理対象となっている全てのコンピュータについて、各コンピュータを特定するための情報を保有するソフトウェア資産管理リスト200とにもとづいて、ネットワーク接続コンピュータリスト100に存在し、かつ、ソフトウェア資産管理リスト200に存在しないコンピュータを抽出し、ソフトウェア資産管理漏れのコンピュータのリスト300を作成することを特徴とするネットワークを利用したソフトウェア資産管理漏れ検出方法。

【選択図】 図1



特願 2 0 0 2 - 3 4 2 7 3 5

出 願 人 履 歴 情 報

識別番号

[ 0 0 0 0 0 4 2 3 7 ]

1 . 変更年月日

1 9 9 0 年 8 月 2 9 日

[変更理由]

新規登録

住 所

東京都港区芝五丁目 7 番 1 号

氏 名

日本電気株式会社

特願 2 0 0 2 - 3 4 2 7 3 5

出 願 人 履 歴 情 報

識別番号

[ 3 9 0 0 0 1 3 9 5 ]

1. 変更年月日

2 0 0 1 年 1 1 月 2 8 日

[変更理由]

名称変更

住 所

大阪府大阪市中央区城見 1 丁目 4 番 2 4 号

氏 名

エヌイーシーシステムテクノロジー株式会社